þÿ"We turn the cube and it twists us : Rubikin ryh

Lahdenperä, Juulia

2015

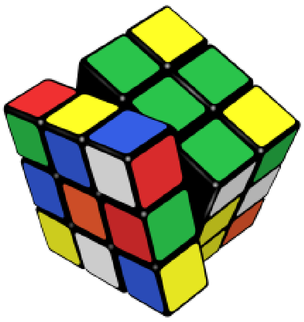
þÿLahdenperä, J 2015, ' "We turn the cube and it twists us : Rubikin r
'.

http://hdl.handle.net/10138/320620

”We turn the cube and it twists us”

Rubikin ryhmän kompositiojono

Juulia Lahdenperä



Kandidaatintutkielma
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto
Ohjaaja FT Jokke Häsä

30. tammikuuta 2015

Tiivistelmä

Tässä työssä määritetään Rubikin kuution symmetriaryhmän kompositiojono ryhmäteorian työkalujen avulla. Luvussa 1 käydään läpi Rubikin kuution taustaa. Luvussa 2 kuutiota tarkastellaan ryhmäteoreettisesta näkökulmasta ja esitellään luvussa 3 tarvittavia käsitteitä ja lauseita. Luvussa 3 määritetään Rubikin kuution kompositiojono tarkastelemalla erikseen kuution paikka- ja asentoryhmiä.

Rubikin kuutio on yksi maailman suosituimmista pulmapeleistä. Sen kehittäjä unkarilainen Ernő Rubik onkin tokaissut: "We turn the cube and it twists us." Aivojumpan lisäksi Rubikin kuutio taipuu ryhmäteorian keskeisten käsitteiden havainnollistamiseen. Kuution siirtoja eli tahkojen pyöräytyksiä voidaan ajatella permutaatioina, jolloin niitä on mahdollista käsitellä algebrallisin menetelmin.

Rubikin ryhmä $\mathbb{R}$ on kuution kaikkien mahdollisten siirtojen muodostama joukko. Rubikin ryhmään kuuluvat siis kuution perussiirrot, sekä näiden kaikki kombinaatiot. Rubikin ryhmällä $\mathbb{R}$ on osajoukko, johon kuuluvat kaikki sellaiset permutaatiot, jotka pitävät kuution palat paikoillaan vaikka voivatkin muuttaa niiden asentoa. Tätä osajoukkoa kutsutaan Rubikin asentoryhmäksi $\mathbb{R}_a$. Rubikin asentoryhmä on Rubikin ryhmän normaali aliryhmä. Sen suhteen muodostettua tekijäryhmää kutsutaan Rubikin paikkaryhmäksi $\mathbb{R}_p$. Paikkaryhmän alkiot liikuttavat kuution paloja niiden asennoista välittämättä. Kuution eräs mahdollinen ratkaisustrategia perustuukin tähän jaotteluun: laitetaan ensin palat oikeille paikoilleen, minkä jälkeen ne voidaan kääntää oikeisiin asentoihin.

Tässä tutkielmassa Rubikin ryhmän $\mathbb{R}$ rakennetta havainnollistetaan syvällisemmin tutkimalla sen sisältämien normaalien aliryhmien muodostamaa jonoa. Pisintä mahdollista jonoa kutsutaan kompositiojonoksi, ja sen peräkkäisistä jäsenistä muodostettua tekijäryhmää jonon kompositiotekijäksi. Kompositiojono vastaa kokonaislukujen alkutekijähajotelmaa, ja ryhmän kompositiotekijät ovat järjestystä vaille yksikäsitteiset. Rubikin ryhmän $\mathbb{R}$ kompositiojonon määrittämisessä keskeisiä menetelmiä ovat permutaatioiden parillisuuden tarkastelu sekä ainoastaan nurkka- tai särmäpaloja liikuttavien permutaatioiden tutkiminen. Näiden avulla muodostetaan jo löydetyille tekijöille aina uusia normaaleja aliryhmiä, kunnes vastaavista tekijäryhmistä tulee lopulta yksinkertaisia. Lopuksi kaikki löydetyt normaalit aliryhmät nostetaan tekijäryhmästä kanonisen surjektion avulla takaisin alkuperäiseen ryhmään. Näin edeten saadaan Rubikin kuutiolle muodostettua kompositiojono, jonka kompositiotekijät ovat kahdeksan alkion joukon alternoiva ryhmä A_8, kahdentoista alkion joukon alternoiva ryhmä A_{12}, kahden alkion syklinen ryhmä C_2 (12 kertaa) sekä kolmen alkion syklinen ryhmä C_3 (7 kertaa).

Sisältö

Otsikon sitaatti (Tran, 2005).

1 Taustaa

Rubikin kuutio on ehkä yksi maailman kuuluisimmista pulmapeleistä. Sen on kehittänyt vuonna 1974 unkarilainen arkkitehti ja kuvanveistäjä Ernő Rubik (s. 1944), joka kutsui kuutiota alunperin nimellä *Bűvös Kocka*, taikakuutio (engl. *the Magic Cube*). Rubik halusi leikkiä geometrisilla muodoilla ja liikutella pikkukuutioita ilman, että iso kuutio hajoaa. Myöhemmin kuution kaupallistamisprosessin yhteydessä se nimettiin uudelleen *Rubikin kuutioksi* kunnianosoitukseksi kehittäjälleen.

> It was wonderful, to see how, after only a few turns, the colors became mixed [$\cdots$] After a while I decided [$\cdots$] let us put the cubes back in order. And it was at that moment that I came face to face with the Big Challenge: What is the way home?
>
> – Ernő Rubik, 1974

Rubikin kuutiolla on $43,252,003,274,489,856,000 \approx 4,3 \cdot 10^{19}$ mahdollista asentoa, joista vain yksi on oikea. Onkin laskettu, että jos maailman jokainen ihminen kääntäisi samaa kuutiota satunnaisesti kerran sekunnissa, kuutio olisi ratkaistuna alkuperäisessä asennossaan noin kolmen vuosisadan välein. Tämän ymmärtää jokainen Rubikin kuution ratkaisemista yrittänyt – sen epämääräisellä kääntelyllä ei pääse ratkaisussa puusta pidemmälle.

Rubikin kuutioita on olemassa erikokoisia: 2×2 -taskukuutio, yleisin 3×3 -kuutio, 4×4 -kuutio, joka on nimetty *Rubikin kostoksi*, 5×5 -kuutio, sekä 6×6- ja 7×7 -kuutiot. Kuutiosta on tietokoneen avulla muodostettu myös useampi kuin 3-ulotteisia versioita. Lisäksi kuutiosta on kehitetty useita muita samantyyppisiä pulmapelejä, kuten numerokuutioita, -palloja ja muita geometrisia muotoja. Tämän tutkielman puitteissa käsittelemme yleisintä 3×3 -kuutiota. Käsitteet ja suurimmilta osin myös ratkaisualgoritmit ovat kuitenkin sovellettavissa myös kuution muille versioille.

Rubikin 3×3 -kuutio koostuu kuudesta erivärisestä tahkosta, joista jokainen sisältää yhdeksän pienempää kuutiota. Näistä neljä on kulmapaloja, neljä reunapaloja ja yksi keskipala. Kuution väritys voi vaihdella, vaikka useimmiten törmää kuutioon, jossa värit ovat sininen, punainen, keltainen, valkoinen, vihreä ja oranssi – jos kuutiota katsotaan sen sinisen sivun suunnasta keltainen väri ylhäällä ja valkoinen sitä vastapäätä alhaalla, muut värit kiertävät kuutiota myötäpäivään järjestyksessä sininen, punainen, vihreä ja oranssi. Kuution ratkaisemisen kannalta värien järjestyksellä ei luonnollisesti ole mitään merkitystä.

Rubikin kuution alkutilassa jokainen tahko on yksivärinen. Tahkoja voidaan pyörittää keskipisteensä ympäri, jolloin värit sekoittuvat. Kuution ratkaiseminen tarkoittaa tahkojen palauttamista takaisin yksivärisiksi. On syytä huomata, että missään siirroissa tahkon keskipalat eivät liiku. Niiden avulla on siis helppo määrittää kunkin tahkon alkuperäinen väri.

Rubikin kuutio on innoittanut monia kilpailemaan sen ratkaisemisnopeudessa. Todelliset taitajat öljyävät kuutioitaan mahdollisimman sulavien tahkon kiertojen aikaansaamiseksi. *World Cube Association* järjestää kilpailuja ja pitää kirjaa maailmanennätyksistä. Kilpasarjoja on kaiken kokoisille Rubikin kuutioille, ja niitä ratkotaan myös sokkona ja jaloilla. Tällä hetkellä 3×3 -kuution on nopeimmin ratkaissut alankomaalainen Mats Valk 5,55 sekunnissa (2013), 4×4 -kuution saksalainen Sebastian Weyer 24,33 sekunnissa (2014) ja 5×5 -kuution australialainen Felix Zemdegs 50,50 sekunnissa (2013). Sokkona 3×3 -kuution on nopeimmin ratkaissut puolalainen Marcin Zalewski 23,68 sekunnissa (2014). (WCA)

Rubikin kuutiossa riittää edelleen pohdittavaa myös matemaatikoille. Kuution ratkaisemiseen tarvittava pienin mahdollinen perussiirtojen eli sivutahkojen neljännesympyrän pyöräytysten määrä vaatii vielä tarkennusta. On osoitettu, että minkä tahansa kuution aseman ratkaisemiseen tarvitaan enintään 29 siirtoa, ja on löydetty asema, jonka ratkaisemiseen tarvitaan vähintään 26 siirtoa. Kaikista täydellisintä algoritmia ei siis ole vielä löytynyt. Jos sivutahkon 180°:en pyöräytys lasketaan myös perussiirroksi, tarvittavien siirtojen määrä on tasan 20. (Rokicki et al, 2010)

2 Rubikin kuution matemaattinen tausta

Ryhmäteoria tutkii algebrallisia rakenteita, joita kutsutaan ryhmiksi. Muut algebran keskeiset käsitteet kuten renkaat, kunnat ja vektoriavaruudet voidaan tulkita ryhmiksi, joille on määritelty tiettyjä lisäominaisuuksia. Nämä rakenteet toistuvat eri matematiikan osa-alueissa, ja näin ollen ryhmäteorialla on merkittävä rooli algebran lisäksi myös muissa matematiikan osa-alueissa.

Rubikin kuutiota voidaan lähestyä ryhmäteorian näkökulmasta. Sitä varten täytyy määritellä muutamia käsitteitä. Nämä käsitteet ja niihin liittyvät tulokset perustuvat pääosin lähteeseen Häsä, 2010a.

2.1 Permutaatiot

Määritelmän mukaan joukon permutaatio on bijektio joukolta itselleen. Se kuvaa joukon sisäistä muutosta, ja tietyssä mielessä permutaatio onkin joukon alkioiden uudelleenjärjestelyä. Permutaatiota voidaan ajatella joko tietyn operaation lopputuloksena tai vaihtoehtoisesti sinä operaationa, joka tähän alkioiden uuteen järjestykseen johtaa. Molemmat ajattelutavat ovat yhtä oikein, joskin tietyissä tilanteissa toinen voi olla toista suotuisampi.

Permutaatiot ovat kuvauksia, joten niiden laskutoimituksena on kuvausten yhdistäminen. Neutraalialkiona on identtinen kuvaus id, ja permutaation σ käänteisalkiona on sen käänteiskuvaus σ^{-1}. Permutaatioilla lasketaan kuten kuvauksilla − ensin oikeanpuoleinen ja sitten vasemmanpuoleinen permutaatio. Permutaatioiden σ ja τ tulo on siis $\sigma\tau = \sigma \circ \tau$.

2.2 Symmetrinen ryhmä ja syklit

Lukujoukolla $N_n = \{1, 2, 3, \ldots, n\}$ on yhteensä $n!$ permutaatiota. Tämä nähdään tuloperiaatteen avulla: ensimmäiselle alkiolle voidaan valita paikka n:llä eri tavalla, toiselle alkiolle $(n-1)$:llä eri tavalla jne. Nyt voidaan määritellä symmetrinen ryhmä S_n, joka muodostuu kaikista joukon N_n permutaatioista.

Määritelmä 2.1. *Symmetrinen ryhmä* S_n on kaikkien joukon N_n permutaatioiden muodostama ryhmä. Ryhmän laskutoimituksena on kuvausten yhdistäminen, neutraalialkiona identtinen kuvaus id ja alkion $\sigma \in S_n$ käänteisalkiona sen käänteiskuvaus σ^{-1}.

Jokainen äärellinen joukko voidaan numeroida varustamalla sen alkiot järjestysnumerolla. Näin ollen minkä tahansa äärellisen joukon permutaatio on jokin joukon N_n permutaatio. Lisäksi jokainen äärellinen ryhmä on isomorfinen jonkin permutaatioryhmän kanssa. Siispä symmetristen ryhmien S_n ominaisuuksien tarkasteleminen riittää kaikkien äärellisten ryhmien tuntemiseen.

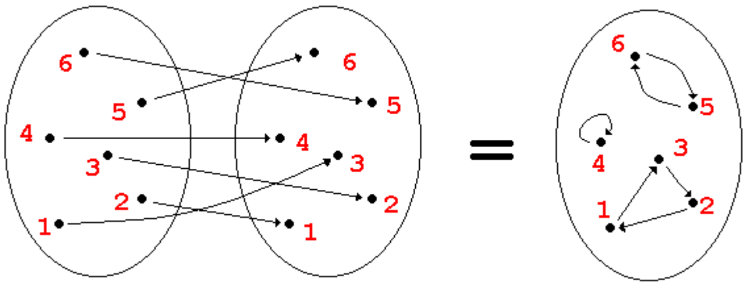
Kuten aikaisemmin mainittiin, permutaatiot ovat kuvauksia. Seuraavassa esimerkissä käydään läpi permutaatioiden merkintätapaa.

Esimerkki 2.2. Olkoon permutaatio $\sigma \in S_6$ sellainen, että $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$, $\sigma(4) = 4$, $\sigma(5) = 6$ ja $\sigma(6) = 5$. Tätä permutaatiota voidaan nyt merkitä seuraavasti:

$$
\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) & \sigma(6) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 132 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix} \begin{pmatrix} 56 \end{pmatrix} = \begin{pmatrix} 132 \end{pmatrix} \begin{pmatrix} 56 \end{pmatrix}.
\end{aligned}
$$

Permutaatio σ on esitetty myös kuvassa 1. *Syklit* ovat permutaatioita, jotka kuvaavat joitain alkioita kehässä toisilleen, eivätkä vaikuta muihin ryhmän alkioihin. Esimerkkimme permutaatio σ koostuu kolmesta erillisestä syklistä: sykleistä $1 \mapsto 3 \mapsto 2 \mapsto 1$, $4 \mapsto 4$ ja $5 \mapsto 6 \mapsto 5$. Näitä syklejä merkitään lyhyesti (132), (4) ja (56). On sovittu, ettei yhden alkion pituisia syklejä tarvitse erikseen kirjoittaa. Tapauksessa, jossa permutaatio on identtinen eli koostuu pelkästään yhden alkion pituisista sykleistä, yksi sykleistä jätetään näkyviin. Tämä sykli on yleensä (1). Siis permutaatio $\sigma = (132)(56)$.

Kuva 1: Esimerkin 3.2 permutaatio σ.



Syklin kertalukua kutsutaan syklin pituudeksi. Esimerkiksi sykli (132) on 3-sykli, sillä se koostuu kolmesta toisilleen kuvautuvasta alkiosta. Yleisesti syklin σ pituus on pienin $n \in \mathbb{N}$, jolle pätee $\sigma^n(x) = x$ kaikilla sykliin kuuluvilla alkioilla x. Syklejä, joiden pituus on kaksi, kutsutaan vaihdoiksi. Itse asiassa jokainen äärellisen joukon permutaatio voidaan muodostaa vaihtojen tulona. Siispä vaihdot virittävät symmetrisen ryhmän S_n. Permutaatiot voidaan jakaa parillisiin ja parittomiin permutaatioihin sen mukaan, tarvitaanko niiden kirjoittamiseen parillinen vai pariton määrä vaihtoja. Esimerkiksi kolmisykli $(132) = (13)(32)$ voidaan kirjoittaa kahden vaihdon tulona. Se on siis parillinen permutaatio.

2.3 Tekijäryhmät

Tekijäryhmät ovat algebrallisia rakenteita, joiden avulla monimutkainen ryhmä voidaan jakaa suurempiin ja yksinkertaisempiin kokonaisuuksiin. Tekijäryhmiä käsiteltäessä unohdetaan hetkeksi ryhmän tarkat yksityiskohdat ja keskitytään sen yleisemmän tason ominaisuuksiin. Myöhemmin voidaan tekijäryhmistä taas palata takaisin tarkastelemaan alkuperäistä ryhmää ja sen ominaisuuksia. Tekijäryhmien tarkastelemiseksi määritellään ensin kaksi muuta käsitettä, vasemmat ja oikeat sivuluokat sekä normaalit aliryhmät.

Määritelmä 2.3. Olkoon G jokin ryhmä, jolla on aliryhmä H. Kullakin alkiolla $g \in G$ määritellään H:n *vasen sivuluokka* $gH = \{gh \mid h \in H\}$. Vastaavasti voidaan määritellä *oikea sivuluokka* $Hg = \{hg \mid h \in H\}$.

Määritelmä 2.4. Ryhmän G aliryhmää H kutsutaan *normaaliksi aliryhmäksi*, jos sen vasemman- ja oikeanpuoleiset sivuluokat ovat samat, eli kaikilla $g \in G$ pätee $gH = Hg$. Tällöin merkitään $H \trianglelefteq G$.

Usein aliryhmän osoittaminen normaaliksi on suoraviivaisempaa alla esiteltävän normaalisuuskriteerin avulla. Normaalisuuskriteeriä tullaan käyttämään useasti Rubikin kuution kompositiojonon selvittämiseksi.

Lause 2.5. *Olkoon G ryhmä ja H sen aliryhmä. Aliryhmä H on normaali täsmälleen silloin, kun kaikilla $g \in G$ pätee $gHg^{-1} \subset H$ eli $ghg^{-1} \in H$ jokaisella $h \in H$.*

Todistus. Ryhmä on normaali, jos kaikilla $g \in G$ pätee $gH = Hg$. Kun yhtälön molemmilla puolilla olevien joukkojen alkiot kerrotaan oikealta g:n käänteisalkiolla, saadaan joukkoyhtälö $H = gHg^{-1}$. Tämä yhtälö pätee siis kaikilla $g \in G$ täsmälleen silloin, kun H on normaali. Tästä nähdään heti, että jos H on normaali, niin myös $gHg^{-1} \subset H$ pätee kaikilla $g \in G$.

Oletetaan sitten, että $g^{-1}Hg \subset H$ pätee kaikilla $g \in G$. Olkoot $h \in H$ ja $g \in G$. Nyt myös $g^{-1} \in G$, joten oletuksen mukaan $g^{-1}h(g^{-1})^{-1} = g^{-1}hg \in H$. Edelleen $h = gg^{-1}hgg^{-1} \in gHg^{-1}$, mistä seuraa, että $H \subset gHg^{-1}$. Näin ollen $H = gHg^{-1}$ kaikilla $g \in G$, ja H on normaali. (Häsä, 2010b: Lause 3.4) $\square$

Nyt voidaan määritellä tekijäryhmä. Tähän määritelmään palataan tuota pikaa Rubikin asentoryhmän yhteydessä.

Määritelmä 2.6. Olkoon $H \trianglelefteq G$. Ryhmää, jonka alkioita ovat sivuluokat gH, missä $g \in G$, kutsutaan *tekijäryhmäksi.* Tekijäryhmän laskutoimituksena on $g_1H \cdot g_2H = (g_1g_2)H$. Tekijäryhmää merkitään G/H.

Tekijäryhmän laskutoimituksen olemassaolon todistamisessa tarvitaan aliryhmän normaalisuutta.

2.4 Rubikin ryhmä

Kuten edellä mainittiin, joukon permutaatio järjestää joukon alkiot uudelleen. Rubikin kuutiossa tahkoja pyörittämällä ruutujen paikat sekoittuvat keskenään. Keskipalojen voidaan ajatella pysyvän paikallaan kaikissa siirtosarjoissa. Numeroimalla eriväristen tahkojen jokainen ruutu keskipaloja lukuun ottamatta Rubikin kuutiota voidaan tarkastella joukkona N_{48}. Tietty kuution siirto vastaa siis tiettyä joukon N_{48} permutaatiota eli ryhmän S_{48} alkiota. Ryhmän S_{48} alkioita on yhteensä $48! \approx 1{,}24 \cdot 10^{61}$ kappaletta. Kuitenkaan kaikkia joukon S_{48} permutaatioita ei voida muodostaa kuution siirroilla. Esimerkiksi sinisen ja valkoisen sivun reunassa olevaa särmäpalan valkoista ruutua ei voi vaihtaa sinisen ja punaisen sivun reunan särmäpalan sinisen sivun ruudun kanssa, sillä tällöin kuutioon tulisi särmäpala, jossa olisi kaksi sinistä ruutua. Tällaista palaa ei kuutiossa ole, jolloin kyseessä ei ole mahdollinen kuution siirto. Ryhmän S_{48} alkioista moni muukin on mahdoton toteuttaa Rubikin kuution avulla. Erilaisia mahdollisia kuution siirtoja onkin ”vain” noin $4{,}3 \cdot 10^{19}$ kappaletta.

Tutkitaan seuraavaksi Rubikin kuution kaikkien mahdollisten siirtojen joukkoa. Se on itse asiassa ryhmä, sillä suoritettaessa kaksi mahdollista siirtoa peräkkäin tulos on edelleen mahdollinen siirto. Se, ettei tehdä lainkaan siirtoa, vastaa identtistä permutaatiota id. Lisäksi minkä tahansa siirron voi peruuttaa kääntämällä tahkoja päinvastaisessa järjestyksessä. Siis mahdollisten siirtojen käänteissiirrot ovat myös mahdollisia siirtoja. Tätä ryhmää kutsutaan *Rubikin ryhmäksi*. Se on symmetrisen ryhmän S_{48} aliryhmä.

Määritelmä 2.7. Olkoon X joukko, johon kuuluvat kaikki Rubikin kuution ruudut keskiruutuja lukuun ottamatta. *Rubikin ryhmä* $\mathbb{R}$ on sellainen joukon X permutaatioiden joukko, jonka jokainen alkio vastaa jotakin Rubikin kuution laillista siirtoa.

Rubikin ryhmä koostuu niin sanotuista *perussiirroista* ja niiden erilaisista kombinaatioista. Se on siis perussiirtojen virittämä. Perussiirrolla tarkoitetaan tietyn tahkon pyörähdystä neljännesympyrän verran myötäpäivään. Laillisilla siirroilla sekoitettua Rubikin kuution ruutujen järjestystä kutsutaan kuution *tilaksi*. Jos tiettyyn tilaan johtaneen kuution siirtojen sarja eli permutaatio on selvillä, kuutio voidaan ratkaista käyttämällä tämän permutaation käänteisalkiota. Ongelmana on vain se, että tiettyä tilaa vastaavan permutaation määrittäminen ja palauttaminen takaisin perussiirroiksi on suhteellisen hankalaa. Senpä vuoksi Rubikin kuution ratkaisemiseksi on kehitetty erilaisia algoritmeja, joilla mikä tahansa kuution tila voidaan ratkaista.

Rubikin kuutiolla voidaan suorittaa myös sellaisia siirtosarjoja, jotka pitävät kuution kaikki palat paikoillaan vaikka muuttavatkin niiden asentoa. Unohdetaan palojen asennot hetkeksi ja tarkastellaan seuraavaksi sellaista Rubikin ryhmän osajoukkoa $\mathbb{R}_a$, johon kuuluvat kaikki ne permutaatiot, jotka pitävät kuution jokaisen palan paikallaan.

Lause 2.8. *Osajoukko $\mathbb{R}_a$ on Rubikin ryhmän normaali aliryhmä.*

Todistus. Rubikin ryhmän osajoukko $\mathbb{R}_a$ on sen aliryhmä. Jos nimittäin molemmat permutaatiot $\sigma \in \mathbb{R}_a$ ja $\tau \in \mathbb{R}_a$ pitävät kaikki palat paikoillaan, niin myös niiden yhdistelmä $\sigma\tau$ ei liikuta kuution paloja. Siis myös $\sigma\tau \in \mathbb{R}_a$. Koska identtinen kuvaus id pitää kaikki palat paikoillaan, niin myös $id \in \mathbb{R}_a$. Lisäksi jos permutaatio σ pitää kaikki palat paikoillaan, ei myöskään sen käänteiskuvaus σ^{-1} niitä liikuta. Siis $\mathbb{R}_a \leq \mathbb{R}$.

Todistetaan seuraavaksi, että aliryhmä $\mathbb{R}_a$ on normaali. Olkoot $\tau \in \mathbb{R}_a$ ja $\sigma \in \mathbb{R}$. Tutkitaan nyt yhdistelmää $\sigma\tau\sigma^{-1}$. Jos σ siirtää jotkin palat toisiin paikkoihin, σ^{-1} siirtää ne takaisin alkuperäisille paikoilleen. Koska τ ei muuta palan paikkaa, ei myöskään koko yhdistelmä sitä tee. Näin ollen $\sigma\tau\sigma^{-1} \in \mathbb{R}_a$ ja $\mathbb{R}_a$ on normaali. (Häsä, 2010b: Lause 3.8) □

Kutsutaan ryhmää $\mathbb{R}_a$ *Rubikin asentoryhmäksi.* Koska se on Rubikin ryhmän normaali aliryhmä, voidaan sen suhteen määrittää tekijäryhmä $\mathbb{R}_p = \mathbb{R}/\mathbb{R}_a$. Kutsutaan tätä tekijäryhmää *Rubikin paikkaryhmäksi.* Rubikin paikkaryhmää voidaan ajatella permutaatioryhmänä, joka liikuttaa kuution paloja niiden asennoista välittämättä. Tekijäryhmien ominaisuuksien mukaisesti on mahdollista ensin tarkastella Rubikin kuutiota Rubikin paikkaryhmän näkökulmasta ja sitten palata kuution yksityiskohtaisempaan tarkasteluun Rubikin asentoryhmässä. Nyt Rubikin kuutiolle voidaan muodostaa ratkaisustrategia: toimitaan ensin Rubikin paikkaryhmässä laittaen kaikki palat oikeille paikoilleen, minkä jälkeen siirrytään Rubikin asentoryhmään kääntämään palat oikeisiin asentoihin. Toisin päin tässä ei olisi mitään järkeä: palalle ei voida mielekkäästi määritellä oikeaa asentoa, jos se ei ole omalla paikallaan.

Tarkastellaan seuraavaksi kuinka tämä käytännössä tapahtuu. Kaikki parilliset permutaatiot muodostavat *alternoivan ryhmän,* jota merkitään $A_n = \{\sigma \in S_n \mid \sigma \text{ on parillinen permutaatio}\}$. Alternoiva ryhmä A_n on symmetrisen ryhmän S_n normaali aliryhmä. Lisäksi se on kolmisyklien virittämä. Tämä tarkoittaa sitä, että kaikki parilliset permutaatiot voidaan muodostaa kolmisyklien tulona.

Rubikin kuution paikkaryhmässä nurkkapalojen ratkaisemiseen tarvittava siirtosarja on joko parillinen tai pariton permutaatio. Parillisessa tapauksessa se ratkeaa kolmisyklien tulona. Tarvittavan siirtosarjan ollessa pariton voidaan tehdä mikä tahansa perussiirto, jolloin ratkaisu muuttuu taas parilliseksi. Tämä johtuu siitä, että perussiirto on pariton permutaatio, ja kahden parittoman permutaation tulo on parillinen. Kun nurkkapalat ovat paikoillaan, myös särmäpalat ovat parillisessa permutaatiossa (kts. 3.5) ja ne saadaan paikoilleen kolmisykleillä. Näin ollen koko Rubikin paikkaryhmä voidaan ratkaista kolmisyklien avulla.

Permutaatiot kuvaavat operaatiota jossain joukossa. Kolmisykli (132) kuvaa operaatiota esimerkiksi joukossa $A = \{1, 2, 3, 4, 5, 6\}$. *Konjugointi* tarkoittaa jossakin joukon osassa toimivan operaation siirtämistä joukon toiseen osaan. Konjugoimalla alkiota $(132) \in A$ alkiolla $(124) \in A$, eli kertomalla se vasemmalta puolelta alkiolla itsellään ja oikealta puolelta sen käänteisalkiolla, saadaan seuraava laskutoimitus:

$$(124)(132)(421) = (1)(234) = (234).$$

Siis joukon A operaatio (132) muuttui joukon A toiseksi operaatioksi (234). Rubikin kuutiossa tämä tarkoittaa sitä, että tietyssä kuution osassa toimivaa opittua siirtosarjaa voidaan konjugoimalla käyttää myös kuution muissa osissa. Tämä vähentää opeteltavien siirtosarjojen määrää huomattavasti. Näin ollen se luo pohjan kuution ratkaisemisessa käytettävien algoritmien muodostamiselle.

3 Rubikin ryhmän kompositiojono

Tutkitaan seuraavaksi hieman syvällisemmin Rubikin ryhmän rakennetta pilkkomalla se pienempiin osiin ja tutkimalla näiden osien ominaisuuksia. Tämä auttaa koko ryhmän tuntemisessa. Luonnollinen tapa jakaa ryhmä osiin on tutkia sen normaaleja aliryhmiä ja muodostaa niiden suhteen tekijäryhmiä. Pilkkomista voidaan jatkaa edelleen etsimällä sekä aliryhmälle että sen suhteen muodostetulle tekijäryhmälle uusia normaaleja aliryhmiä, jolloin saadaan taas uusia tekijäryhmiä. Koska Rubikin ryhmä on äärellinen, jossain vaiheessa päädytään ryhmään, jolla ei enää ole epätriviaalia normaalia aliryhmää. Nyt löydetyistä ryhmän normaaleista aliryhmistä saadaan muodostettua jono, jonka tekijöitä kutsutaan ryhmän kompositiotekijöiksi. Määritellään tämä vielä täsmällisesti. Merkitään sitä varten n-alkioista syklistä ryhmää C_n ja triviaalia ryhmää 1.

Määritelmä 3.1. (Häsä, 2010a) Ryhmän G *normaali jono* on jono aliryhmiä G_i, joille pätee

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1.$$

Tekijäryhmiä G_i/G_{i+1} kutsutaan jonon *tekijöiksi*. Tekijöitä tarkastellessa keskenään isomorfiset ryhmät tulkitaan samoiksi. Jonon *pituus* on jonon aitojen inkluusioiden määrä, joka on sama kuin epätriviaalien tekijöiden määrä.

Ryhmällä voi olla useita normaaleja jonoja. Esimerkiksi kahdentoista alkion syklisellä ryhmällä on normaalit jonot $C_{12} \triangleright C_6 \triangleright 1$ ja $C_{12} \triangleright C_4 \triangleright 1$, joilla on eri tekijät C_2 ja C_6 sekä C_3 ja C_4. Näitä jonoja voidaan kuitenkin laajentaa lisäämällä niihin uusia normaaleja aliryhmiä. Tätä kutsutaan jonon *hienontamiseksi.*

Määritelmä 3.2. (Häsä, 2010a) Normaalia jonoa (H_i) sanotaan jonon (G_i) *hienonnukseksi*, mikäli se sisältää kaikki jonon (G_i) jäsenet, eli jono (G_i) on jonon (H_i) osajono.

Esimerkiksi jono $C_{12} \triangleright C_6 \triangleright C_3 \triangleright 1$ on jonon $C_{12} \triangleright C_6 \triangleright 1$ hienonnus. Kun normaaliin jonoon lisätään uusia aliryhmiä, tulee jossain vaiheessa vastaan tilanne, jossa uusia (epätriviaaleja) aliryhmiä ei enää löydy. Tällaista pisintä mahdollista normaalia jonoa, joka ei sisällä triviaaleja tekijöitä, kutsutaan *kompositiojonoksi.*

Määritelmä 3.3. (Häsä, 2010a) Jos ryhmän normaalilla jonolla ei ole triviaaleja tekijöitä, mutta kaikilla sen hienonnuksilla on, jonoa kutsutaan ryhmän *kompositiojonoksi.*

Kompositiojono jakaa ryhmän yksinkertaisempiin osiin ja se vastaakin tietyssä mielessä kokonaislukujen alkutekijähajotelmaa. Ryhmän kompositiotekijät ovat järjestystä vaille yksikäsitteiset. Esimerkiksi ryhmällä C_{12} on kolme kompositiojonoa $C_{12} \triangleright C_6 \triangleright C_3 \triangleright 1$, $C_{12} \triangleright C_6 \triangleright C_2 \triangleright 1$ ja $C_{12} \triangleright C_4 \triangleright C_2 \triangleright 1$, joiden tekijät ovat järjestyksessä C_2, C_2 ja C_3, C_2, C_3 ja C_2 sekä C_3, C_2 ja C_2. Alkutekijähajotelmasta poiketen kahdella ryhmällä voi kuitenkin olla samat kompositiotekijät, vaikka ryhmät eivät olekaan keskenään isomorfisia. Nimittäin Kleinin neliryhmällä K_4 on kompositiojono $K_4 \triangleright C_2 \triangleright 1$, jonka tekijät ovat C_2 ja C_2. Samat tekijät löytyvät myös neljän alkion syklisen ryhmän C_4 kompositiojonosta $C_4 \triangleright C_2 \triangleright 1$, vaikka ryhmät eivät ole isomorfisia keskenään.

Seuraava lause osoittautuu hyödylliseksi kompositiojonon muodostamisessa. Sen nojalla riittää tutkia normaalin jonon tekijöiden yksinkertaisuutta. Ryhmää kutsutaan yksinkertaiseksi, jos se on epätriviaali eikä sillä ole aitoja epätriviaaleja normaaleja aliryhmiä.

Lause 3.4. *Ryhmän G normaali jono on kompositiojono, jos ja vain jos sen tekijät ovat yksinkertaisia.*

Todistus. (Häsä, 2010a) □

Nyt voidaan alkaa määrittämään Rubikin ryhmän kompositiojonoa. Tehdään se tutkimalla Rubikin ryhmän normaaleja aliryhmiä ja niiden suhteen muodostettuja tekijäryhmiä, ja yritetään löytää uusia normaaleja aliryhmiä niin pitkälle kuin mahdollista. Tavoitteena on siis ”rakentaa” Rubikin ryhmä $\mathbb{R}$ sen sisältämistä yksinkertaisista ryhmistä.

3.1 Rubikin paikkaryhmän kompositiojono

Aikaisemmin osoitettiin, että Rubikin ryhmällä $\mathbb{R}$ on normaali aliryhmä Rubikin asentoryhmä $\mathbb{R}_a$. Siispä Rubikin ryhmälle voidaan muodostaa normaali jono $\mathbb{R} \trianglerighteq \mathbb{R}_a \trianglerighteq 1$, jonka ensimmäinen tekijä on Rubikin paikkaryhmä $\mathbb{R}_p = \mathbb{R}/\mathbb{R}_a$. Rubikin paikkaryhmän tutkimiseksi tarvitsemme seuraavan apulauseen. Merkitään sitä varten ainoastaan särmäpaloja liikuttavien permutaatioiden muodostamaa ryhmää $\mathbb{R}_{p(S)}$ ja vastaavasti ainoastaan nurkkapaloja liikuttavien permutaatioiden muodostamaa ryhmää $\mathbb{R}_{p(N)}$. Kutsutaan näitä ryhmiä Rubikin särmä- ja nurkkapalojen paikkaryhmiksi.

Lemma 3.5. *Jos τ on Rubikin paikkaryhmän siirto, niin sille löytyy yksikäsitteinen esitys tulona $\tau = \nu \circ \sigma$, missä $\nu \in \mathbb{R}_{p(N)}$ ja $\sigma \in \mathbb{R}_{p(S)}$. Lisäksi näille permutaatioille pätee* $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma)$.

Todistus. (Häsä, 2010a) □

Näin ollen Rubikin paikkaryhmä $\mathbb{R}_p$ voidaan kahteen osaan sen mukaan, onko paikkaryhmän permutaatio parillisten vai parittomien permutaatioiden tulo. Olkoon $\tau \in \mathbb{R}_p$. Nyt lemman 3.5 nojalla $\tau = \nu \circ \sigma$, missä $\nu \in \mathbb{R}_{p(N)}$ ja $\sigma \in \mathbb{R}_{p(S)}$. Lisäksi näille permutaatioille pätee $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma)$. Jos $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma) = 1$, niin merkitään $\tau \in \mathbb{R}_p^{(1)}$, ja jos $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma) = -1$, niin merkitään $\tau \in \mathbb{R}_p^{(-1)}$. Todistetaan seuraavaksi, että parillisten permutaatioiden muodostamat paikkaryhmän permutaatiot muodostavat Rubikin paikkaryhmän normaalin aliryhmän.

Lause 3.6. *Rubikin paikkaryhmän parillisten permutaatioiden tulopermutaatioiden joukko $\mathbb{R}_p^{(1)}$ on Rubikin paikkaryhmän $\mathbb{R}_p$ normaali aliryhmä.*

Todistus. Osoitetaan ensin, että joukko $\mathbb{R}_p^{(1)}$ on Rubikin paikkaryhmän $\mathbb{R}_p$ aliryhmä. Selvästi $\mathbb{R}_p^{(1)} \subset \mathbb{R}_p$. Lisäksi $\mathbb{R}_p^{(1)} \neq \emptyset$, sillä $id \in \mathbb{R}_p^{(1)}$. Olkoot τ_1 ja τ_2 jotkin Rubikin parillisen paikkaryhmän permutaatiot. Tällöin $\tau_1 = \sigma_1 \circ \nu_1$ ja $\tau_2 = \sigma_2 \circ \nu_2$, missä $\sigma_1, \sigma_2 \in \mathbb{R}_{p(S)}$ ja $\nu_1, \nu_2 \in \mathbb{R}_{p(N)}$, jonka lisäksi $\operatorname{sign}(\sigma_1) = \operatorname{sign}(\sigma_2) = \operatorname{sign}(\nu_1) = \operatorname{sign}(\nu_2) = 1$. Nyt

$$\tau_1\tau_2^{-1} = (\sigma_1\nu_1)(\sigma_2\nu_2)^{-1} = (\sigma_1\nu_1)(\sigma_2^{-1}\nu_2^{-1}) = (\sigma_1\sigma_2^{-1})(\nu_1\nu_2^{-1}) \in \mathbb{R}_p^{(1)},$$

sillä $\operatorname{sign}(\sigma_1\sigma_2^{-1}) = \operatorname{sign}(\nu_1\nu_2^{-1}) = 1 \cdot 1 = 1$. Näin ollen $\mathbb{R}_p^{(1)} \leq \mathbb{R}_p$.

Osoitetaan sitten, että aliryhmä $\mathbb{R}_p^{(1)}$ on normaali Rubikin paikkaryhmässä $\mathbb{R}_p$. Olkoon ρ jokin Rubikin paikkaryhmän permutaatio. Tällöin sille on yksikäsitteinen esitys tulona $\rho = \sigma_\rho\nu_\rho$, missä $\sigma_\rho \in \mathbb{R}_{p(S)}$, $\nu_\rho \in \mathbb{R}_{p(N)}$ ja $\operatorname{sign}(\sigma_\rho) = \operatorname{sign}(\nu_\rho)$. Olkoon τ jokin Rubikin parillisen paikkaryhmän permutaatio. Tällöin pätee $\tau = \sigma_\tau \nu_\tau$, missä $\sigma_\tau \in \mathbb{R}_{p(S)}$, $\nu_\tau \in \mathbb{R}_{p(N)}$ ja $\operatorname{sign}(\sigma_\tau) = \operatorname{sign}(\nu_\tau) = 1$. Nyt

$$\begin{aligned}\rho\tau\rho^{-1} &= (\sigma_\rho\nu_\rho)(\sigma_\tau\nu_\tau)(\sigma_\rho\nu_\rho)^{-1} = (\sigma_\rho\nu_\rho)(\sigma_\tau\nu_\tau)(\sigma_\rho^{-1}\nu_\rho^{-1})\\ &= (\sigma_\rho\sigma_\tau\sigma_\rho^{-1})(\nu_\rho\nu_\tau\nu_\rho^{-1}),\end{aligned}$$

missä $\sigma_\rho\sigma_\tau\sigma_\rho^{-1} \in \mathbb{R}_{p(S)}$ ja $\nu_\rho\nu_\tau\nu_\rho^{-1} \in \mathbb{R}_{p(N)}$. Huomataan, että

$$\operatorname{sign}(\sigma_\rho\sigma_\tau\sigma_\rho^{-1}) = \operatorname{sign}(\sigma_\rho)\operatorname{sign}(\sigma_\tau)\operatorname{sign}(\sigma_\rho^{-1}) = 1 \cdot 1 \cdot 1 = 1$$

tai

$$\operatorname{sign}(\sigma_\rho\sigma_\tau\sigma_\rho^{-1}) = \operatorname{sign}(\sigma_\rho)\operatorname{sign}(\sigma_\tau)\operatorname{sign}(\sigma_\rho^{-1}) = (-1) \cdot 1 \cdot (-1) = 1.$$

Koska $\rho\tau\rho^{-1}$ on Rubikin paikkaryhmän permutaatio, pätee $\operatorname{sign}(\sigma_\rho\sigma_\tau\sigma_\rho^{-1}) = \operatorname{sign}(\nu_\rho\nu_\tau\nu_\rho^{-1}) = 1$. Näin ollen konjugaatin $\rho\tau\rho^{-1}$ tuloesitys muodostuu parillisista permutaatioista, joten $\rho\tau\rho^{-1} \in \mathbb{R}_p^{(1)}$. Siispä $\mathbb{R}_p^{(1)} \trianglelefteq \mathbb{R}_p$.

□

Löydettiin siis uusi normaali aliryhmä $\mathbb{R}_p^{(1)}$, jonka suhteen voidaan edelleen muodostaa tekijäryhmä. Kutsutaan tätä aliryhmää Rubikin parilliseksi paikkaryhmäksi. Osoittautuu, että sen suhteen muodostettu tekijäryhmä on yksinkertainen.

Lause 3.7. *Rubikin paikkaryhmässä Rubikin parillisen paikkaryhmän $\mathbb{R}_p^{(1)}$ suhteen muodostetun tekijäryhmän $\mathbb{R}_p/\mathbb{R}_p^{(1)}$ kertaluku on kaksi, jolloin se on yksinkertainen.*

Todistus. Olkoon π jokin Rubikin paikkaryhmän perussiirto. Tällöin $\pi = \pi_N \circ \pi_S$, missä $\pi_N \in \mathbb{R}_{p(N)}$ ja $\pi_S \in \mathbb{R}_{p(N)}$. Koska kuution perussiirto liikuttaa neljää nurkka- ja särmäpalaa, täytyy päteä $\operatorname{sign}(\pi_N) = \operatorname{sign}(\pi_S) = -1$. Siispä $\pi \notin \mathbb{R}_p^{(1)}$.

Olkoon sitten $\tau = \nu \circ \sigma$, missä $\nu \in \mathbb{R}_{p(N)}$, $\sigma \in \mathbb{R}_{p(S)}$ ja $\tau \notin \mathbb{R}_p^{(1)}$, jolloin $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma) = -1$. Tutkitaan, kuuluvatko permutaatiot π ja τ samaan sivuluokkaan. Koska nurkka- ja särmäpalojen paikkaryhmien permutaatiot liikuttavat erillisiä paloja, niin $\pi^{-1} \circ \tau = (\pi_N \circ \pi_S)^{-1} \circ (\nu \circ \sigma) = (\pi_N^{-1} \circ \nu) \circ (\pi_S^{-1} \circ \sigma)$. Huomataan, että $\operatorname{sign}(\pi_N^{-1} \circ \nu) = \operatorname{sign}(\pi_S^{-1} \circ \sigma) = 1$, jolloin $\pi^{-1} \circ \tau \in \mathbb{R}_p^{(1)}$. Näin ollen π ja τ kuuluvat samaan sivuluokkaan. Siispä tekijäryhmän $\mathbb{R}_p/\mathbb{R}_p^{(1)}$ kertaluku on kaksi. □

Tutkitaan seuraavaksi Rubikin parillisen paikkaryhmän osajoukkoja. Huomataan, että Rubikin nurkkapalojen paikkaryhmä on itse asiassa Rubikin parillisen paikkaryhmän normaali aliryhmä.

Lause 3.8. *Rubikin nurkkapalojen paikkaryhmä $\mathbb{R}_{p(N)}$ on Rubikin parillisen paikkaryhmän $\mathbb{R}_p^{(1)}$ normaali aliryhmä.*

Todistus. Osoitetaan ensin, että $\mathbb{R}_{p(N)} \subset \mathbb{R}_p^{(1)}$. Oletetaan, että τ_N on permutaatio, joka liikuttaa ainoastaan nurkkapaloja eli $\tau_N \in \mathbb{R}_{p(N)}$. Tällöin myös $\tau_N \in \mathbb{R}_p$. Siispä lemman 3.5 nojalla on olemassa yksikäsitteiset permutaatiot $\nu \in \mathbb{R}_{p(N)}$ ja $\sigma \in \mathbb{R}_{p(S)}$, joille pätee $\tau_N = \nu \circ \sigma$. Koska τ_N liikuttaa ainoastaan nurkkapaloja, täytyy päteä $\sigma = id$. Siispä $\tau_N = \nu \circ \sigma = \nu \circ id = \nu$. Nyt lemman 3.5 nojalla pätee myös $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma) = \operatorname{sign}(id) = 1$. Siispä kaikki permutaatiot $\tau_N \in \mathbb{R}_{p(N)}$ ovat parillisten permutaatioiden tuloja, joten $\mathbb{R}_{p(N)} \subset \mathbb{R}_p^{(1)}$. Lisäksi nurkkapalojen permutaatioista muodostettu osajoukko $\mathbb{R}_{p(N)} \neq \emptyset$, sillä $id \in \mathbb{R}_{p(N)}$.

Oletetaan sitten, että permutaatiot α ja β liikuttavat ainoastaan nurkkapaloja, eli $\alpha, \beta \in \mathbb{R}_{p(N)}$. Tällöin myös niiden yhdiste $\alpha \circ \beta$ liikuttaa ainoastaan nurkkapaloja, joten $\alpha \circ \beta \in \mathbb{R}_{p(N)}$. Lisäksi jos permutaatio α liikuttaa ainoastaan nurkkapaloja, samoin tekee myös sen käänteispermutaatio α^{-1}. Siispä kaikille $\alpha \in \mathbb{R}_{p(N)}$ pätee $\alpha^{-1} \in \mathbb{R}_{p(N)}$. Näin ollen $\mathbb{R}_{p(N)} \leq \mathbb{R}_p^{(1)}$.

Osoitetaan sitten, että $\mathbb{R}_{p(N)}$ on normaali ryhmässä $\mathbb{R}_p^{(1)}$. Olkoon $\tau_N \in \mathbb{R}_{p(N)}$ ja $\tau_1 \in \mathbb{R}_p^{(1)}$. Nyt τ_N liikuttaa vain nurkkapaloja, mutta τ_1 voi liikuttaa joko ainoastaan nurkkapaloja tai (näiden lisäksi myös) särmäpaloja.

1. Jos τ_1 liikuttaa vain nurkkapaloja, niin myös sen käänteispermutaatio τ_1^{-1} liikuttaa vain nurkkapaloja. Näin ollen myös konjugaatti $\tau_1 \tau_N \tau_1^{-1}$ liikuttaa ainoastaan nurkkapaloja. Siis $\tau_1 \tau_N \tau_1^{-1} \in \mathbb{R}_{p(N)}$.

2. Tutkitaan sitten tapausta, jossa τ_1 liikuttaakin (nurkkapalojen lisäksi myös) särmäpaloja. Huomataan, että konjugaatti $\tau_1 \tau_N \tau_1^{-1} \in \mathbb{R}_{p(N)}$, sillä kun permutaatio τ_1^{-1} liikuttaa särmäpaloja, keskimmäinen permutaatio τ_N ei niitä liikuta, jolloin τ_1 voi tuoda liikkuneet särmäpalat takaisin alkuperäisille paikoilleen. Loppujen lopuksi ainoastaan nurkkapalat liikkuivat.

Näin ollen konjugaatti $\tau_1 \tau_N \tau_1^{-1}$ liikuttaa vain nurkkapaloja, jolloin $\tau_1 \tau_N \tau_1^{-1} \in \mathbb{R}_{p(N)}$ ja täten $\mathbb{R}_{p(N)} \trianglelefteq \mathbb{R}_p^{(1)}$. □

Tässä kohtaa on hyvä huomata, että Rubikin kuution nurkkapalojen paikkaryhmä $\mathbb{R}_{p(N)}$ on isomorfinen kahdeksanalkioisen alternoivan ryhmän A_8 kanssa.

Ensinnäkin ryhmän $\mathbb{R}_{p(N)}$ kaikki alkiot ovat parillisia permutaatioita ja nurkkapaloja on kuutiossa kahdeksan kappaletta, se on isomorfinen jonkin ryhmän A_8 aliryhmän H kanssa. Lisäksi tiedetään, että alternoiva ryhmä

A_8 on 3-syklien virittämä. Koska mikä tahansa ryhmän $\mathbb{R}_p$ 3-sykli, joka liikuttaa vain nurkkapaloja, on mahdollinen siirto (Häsä, 2010b, Lause 4.10.), niin aliryhmän H kertaluku on sama kuin alternoivan ryhmän A_8 kertaluku. Siispä ne ovat sama ryhmä, jolloin $\mathbb{R}_{p(N)} \cong A_8$.

Tunnetusti alternoiva ryhmä A_8 on yksinkertainen. Siispä Rubikin paikkaryhmällä $\mathbb{R}_{p(N)}$ ei ole epätriviaaleja normaaleja aliryhmiä.

Tutkitaan sitten tekijäryhmää $\mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)}$. Samassa sivuluokassa olevat alkiot liikuttavat samoja särmäpaloja ja eroavat toisistaan vain jonkin nurkkapalojen paikkaryhmän siirron verran. (Tämä kaikki tapahtuu asennoista välittämättä.) Osoitetaan seuraavaksi, että tekijäryhmä $\mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)}$ on isomorfinen särmäpalojen paikkaryhmän $\mathbb{R}_{p(S)}$ kanssa.

Lause 3.9. *Rubikin parillisessa paikkaryhmässä nurkkapalojen paikkaryhmän suhteen muodostettu tekijäryhmä $\mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)}$ on isomorfinen Rubikin särmäpalojen paikkaryhmän $\mathbb{R}_{p(S)}$ kanssa.*

Todistus. Määritellään kuvaus $f : \mathbb{R}_p^{(1)} \to \mathbb{R}_{p(S)}$, $f(\nu \circ \sigma) = \sigma$ kaikilla $\nu \circ \sigma \in \mathbb{R}_p^{(1)}$, missä $\nu \in \mathbb{R}_{p(N)}$ ja $\sigma \in \mathbb{R}_{p(S)}$. Kuvaus f on homomorfismi, sillä

$$f\Big((\nu_1 \circ \sigma_1) \circ (\nu_2 \circ \sigma_2)\Big) = f\Big((\nu_1 \circ \nu_2) \circ (\sigma_1 \circ \sigma_2)\Big) = \sigma_1 \circ \sigma_2 = f(\nu_1 \circ \sigma_1) \circ f(\nu_2 \circ \sigma_2).$$

Tutkitaan sitten kuvauksen f ydintä ja kuvaa. Kuvauksen f ydin on

$$\begin{aligned} Ker f &= \{\nu \circ \sigma \in \mathbb{R}_p^{(1)} \,|\, f(\nu \circ \sigma) = id\} = \{\nu \circ \sigma \in \mathbb{R}_p^{(1)} \,|\, \sigma = id\} \\ &= \{\nu \in \mathbb{R}_p^{(1)} \,|\, \nu \in \mathbb{R}_{p(N)}\} = \mathbb{R}_{p(N)} \end{aligned}$$

ja kuva

$$\begin{aligned} Im(f) &= \{\chi \in \mathbb{R}_{p(S)} \mid f(\nu \circ \sigma) = \chi \text{ jollakin } \nu \circ \sigma \in \mathbb{R}_p^{(1)}\} \\ &= \{\chi \in \mathbb{R}_{p(S)} \mid \sigma = \chi \text{ jollakin } \sigma \in \mathbb{R}_{p(S)}\} = \mathbb{R}_{p(S)}. \end{aligned}$$

Nyt homomorfialauseen nojalla $\mathbb{R}_{p(S)} \cong \mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)}$. □

Edellä siis osoitettiin, että tekijäryhmä $\mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)}$ on isomorfinen särmäpalojen paikkaryhmän $\mathbb{R}_{p(S)}$ kanssa. Huomataan, kuten edellä nurkkapalojen tapauksessa, että särmäpalojen paikkaryhmä $\mathbb{R}_{p(S)}$ on isomorfinen kahdentoista alkion alternoivan ryhmän A_{12} kanssa. Siispä tekijäryhmä $\mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)}$ ja alternoiva ryhmä A_{12} ovat isomorfisia. Koska alternoiva ryhmä A_{12} on yksinkertainen, niin myös tekijäryhmä $\mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)}$ on yksinkertainen.

Näin ollen Rubikin paikkaryhmän $\mathbb{R}_p$ osalta kompositiojono on valmis. Se on muotoa

$$\mathbb{R}_p \trianglerighteq \mathbb{R}_p^{(1)} \trianglerighteq \mathbb{R}_{p(N)} \trianglerighteq 1,$$

jossa ensimmäinen tekijä $\mathbb{R}_p/\mathbb{R}_p^{(1)}$ on yksinkertainen, koska sen kertaluku on kaksi, sekä toinen ja kolmas tekijä $\mathbb{R}_p^{(1)}/\mathbb{R}_{p(N)} \cong \mathbb{R}_{p(S)}$ ja $\mathbb{R}_{p(N)}$ ovat isomorfisia tunnetusti yksinkertaisten ryhmien A_{12} ja A_8 kanssa.

3.2 Rubikin asentoryhmän kompositiojono

Siirrytään seuraavaksi tarkastelemaan Rubikin asentoryhmää $\mathbb{R}_a$. Asentoryhmään kuuluvat kaikki ne Rubikin ryhmän permutaatiot, jotka eivät liikuta paloja mutta voivat muuttaa niiden asentoa. Lähdetään etsimään sille normaaleja aliryhmiä. Osoitetaan kuitenkin ensin, että Rubikin asentoryhmä on vaihdannainen.

Lause 3.10. *Rubikin asentoryhmä $\mathbb{R}_a$ on vaihdannainen.*

Todistus. Olkoot σ, $\tau \in \mathbb{R}_a$. Jos permutaatiot σ ja τ vaikuttavat kuution eri paloihin, niin $\sigma \circ \tau = \tau \circ \sigma$, sillä tällöin palojen kääntöjärjestyksellä ei selvästikään ole merkitystä. Olkoon sitten p sellainen kuution pala, jota molemmat permutaatiot σ ja τ kääntävät. Olkoon luvut $s \in \mathbb{Z}$ permutaation σ ja $t \in \mathbb{Z}$ permutaation τ palaan p tekemien kääntöjen lukumäärä, jossa etumerkki kertoo käännön suunnan. Nyt selvästi $s + t = t + s$ eli palojen kääntöjärjestyksellä ei edelleenkään ole merkitystä. Sama päättely voidaan toistaa mille tahansa palalle, johon molemmat permutaatiot σ ja τ vaikuttavat. Siispä ryhmä $\mathbb{R}_a$ on vaihdannainen. □

Rubikin asentoryhmän vaihdannaisuudesta seuraa, että kaikki ryhmän aliryhmät ovat normaaleja.

Rubikin asentoryhmällä on kaksi osajoukkoa, joiden alkiot kääntävät ainoastaan joko nurkka- tai särmäpaloja. Merkitään niiden permutaatioiden muodostamaa joukkoa, jotka pitävät kaikki palat paikoillaan mutta voivat muuttaa nurkkapalojen asentoa $\mathbb{R}_{a(N)}$. Selvästi se on ryhmä, joten kutsutaan sitä Rubikin nurkkapalojen asentoryhmäksi. Vastaavasti särmäpalojen tapauksessa merkitään $\mathbb{R}_{a(S)}$ niiden permutaatioiden joukkoa, jotka pitävät palat paikoillaan mutta voivat kääntää särmäpaloja, ja kutsutaan sitä Rubikin särmäpalojen asentoryhmäksi.

Rubikin asentoryhmällä on siis normaali jono $\mathbb{R}_a \trianglerighteq \mathbb{R}_{a(N)} \trianglerighteq 1$. Tutkitaan tämän normaalin jonon ensimmäistä tekijää $\mathbb{R}_a/\mathbb{R}_{a(N)}$. Huomataan, että samassa sivuluokassa olevat permutaatiot kääntävät samoja särmäpaloja samalla tavalla, ja ne eroavat toisistaan ainoastaan jonkin nurkkapalojen asentoryhmän permutaation verran. Näin ollen tekijäryhmä $\mathbb{R}_a/\mathbb{R}_{a(N)}$ on isomorfinen särmäpalojen asentoryhmän $\mathbb{R}_{a(S)}$ kanssa. Todistus etenee kuten Rubikin paikkaryhmän vastaavassa tilanteessa (Lause 3.9).

Tutkitaan sitten särmäpalojen asentoryhmää $\mathbb{R}_{a(S)}$ ja sen mahdollisia normaaleja aliryhmiä. Tiedetään, että särmäpaloja on 12 kappaletta. Tavoitteena on muodostaa sisäkkäisiä normaaleja aliryhmiä kiinnittämällä aina enemmän särmäpaloja siten, että tekijäryhmästä tulee lopulta yksinkertainen.

Särmäpalojen asentoryhmällä on osajoukko, joka muodostuu niistä permutaatioista, jotka voivat kääntää kaikkia muita paitsi yhtä särmäpalaa. Merkitään tätä osajoukkoa $\mathbb{R}_{a(S)}(1)$, ja sen kaikissa permutaatioissa paikallaan pysyvää särmäpalaa s_1. Osoitetaan, että tämä osajoukko $\mathbb{R}_{a(S)}(1)$ on Rubikin särmäpalojen asentoryhmän $\mathbb{R}_{a(S)}$ normaali aliryhmä.

Lause 3.11. *Osajoukko $\mathbb{R}_{a(S)}(1)$ on ryhmän $\mathbb{R}_{a(S)}$ normaali aliryhmä.*

Todistus. Selvästi $\mathbb{R}_{a(S)}(1)$ kuuluu joukkoon $\mathbb{R}_{a(S)}$. Oletetaan, että permutaatiot τ ja $\sigma \in \mathbb{R}_{(S)}(1)$ eli ne eivät liikuta särmäpalaa s_1. Tällöin yhdistetty permutaatio $\tau \circ \sigma$ ei myöskään liikuta palaa s_1, jolloin $\tau \circ \sigma \in \mathbb{R}_{a(S)}(1)$. Osajoukko on siis suljettu laskutoimituksen suhteen. Liitännäisyys periytyy ryhmästä $\mathbb{R}_{a(S)}$. Myöskään neutraalialkio ei käännä palaa s_1, joten $id \in \mathbb{R}_{a(S)}(1)$. Lisäksi, jos permutaatio $\sigma \in \mathbb{R}_{a(S)}(1)$ niin myös sen käänteisalkio $\sigma^{-1} \in \mathbb{R}_{a(S)}(1)$. Siispä $\mathbb{R}_{a(S)}(1) \leq \mathbb{R}_{a(S)}$. Koska särmäpalojen asentoryhmä on vaihdannainen, niin tästä seuraa, että $\mathbb{R}_{a(S)}(1)$ on ryhmän $\mathbb{R}_{a(S)}$ normaali aliryhmä. $\square$

Tarkastellaan sitten tekijäryhmää $\mathbb{R}_{a(S)}/\mathbb{R}_{a(S)}(1)$. Huomataan, että se on yksinkertainen. Todistetaan tämä vielä tarkasti.

Lause 3.12. *Tekijäryhmä $\mathbb{R}_{a(S)}/\mathbb{R}_{a(S)}(1)$ on yksinkertainen.*

Todistus. Oletetaan, että permutaatiot σ_1 ja σ_2 kääntävät myös särmäpalaa s_1, jolloin $\sigma_1, \sigma_2 \notin \mathbb{R}_{a(S)}(1)$. Koska särmäpalalla s_1 on vain kaksi mahdollista asentoa, σ_1 ja σ_2 kääntävät sitä samalla tavalla. Näin ollen ne eroavat toisistaan ainoastaan jonkin aliryhmän $\mathbb{R}_{a(S)}(1)$ siirron verran. Siispä ne kuuluvat samaan sivuluokkaan. Tämä tarkoittaa sitä, sivuluokkia on vain kaksi. Näin ollen tekijäryhmän $\mathbb{R}_{a(S)}/\mathbb{R}_{a(S)}(1)$ indeksi on kaksi, ja täten se on yksinkertainen. $\square$

Kiinnitetään seuraavaksi kaksi särmäpalaa s_1 ja s_2, ja tutkitaan niiden särmäpalojen asentoryhmään kuuluvien permutaatioiden muodostamaa osajoukkoa, joissa nämä kaksi palaa pysyvät paikoillaan. Merkitään tätä osajoukkoa $\mathbb{R}_{a(S)}(2)$. Huomataan, että se on ryhmän $\mathbb{R}_{a(S)}(1)$ normaali aliryhmä, ja sen suhteen muodostetun tekijäryhmän indeksi on kaksi (todistukset kuten edellä). Aivan vastaavasti voidaan jatkaa normaalien aliryhmien muodostamista kiinnittämällä aina yksi särmäpala lisää, ja näiden aliryhmien suhteen muodostetuista tekijäryhmistä tulee aina yksinkertaisia. Rubikin kuutiossa ainoastaan yhden särmäpalan kääntyminen (ts. muut 11 särmäpalaa pysyisivät paikoillaan) ei ole mahdollista. Tämä seuraa suoraan Häsä, 2010b lauseesta 6.8. Siispä suurin mahdollinen kiinnitettyjen särmäpalojen lukumäärä on kymmenen.

Näin ollen Rubikin särmäpalojen asentoryhmän $\mathbb{R}_{a(S)}$ kompositiojonoksi saadaan

$$\mathbb{R}_{a(S)} \trianglerighteq \mathbb{R}_{a(S)}(1) \trianglerighteq \mathbb{R}_{a(S)}(2) \trianglerighteq \mathbb{R}_{a(S)}(3) \trianglerighteq \cdots \trianglerighteq \mathbb{R}_{a(S)}(10) \trianglerighteq 1,$$

jonka kaikki tekijät ovat kaksialkioisia yksinkertaisia syklisiä ryhmiä.

Palataan sitten tutkimaan Rubikin nurkkapalojen asentoryhmää $\mathbb{R}_{a(N)}$. Nurkkapaloja on kahdeksan kappaletta, joilla jokaisella on kolme mahdollista asentoa. Edetään aivan vastaavasti kuin särmäpalojen asentoryhmän tapauksessa. Tutkitaan ensin osajoukkoa $\mathbb{R}_{a(N)}(1)$, johon kuuluu kaikki ne nurkkapalojen asentoryhmän permutaatiot, jotka voivat kääntää kaikkia muita paitsi yhtä nurkkapalaa. Merkitään tätä kaikissa siirroissa paikallaan pysyvää nurkkapalaa n_1. Kyseessä on normaali aliryhmä, jonka suhteen muodostetun tekijäryhmän indeksi on kolme (todistukset kuten särmäpalojen tapauksessa). Näin ollen tekijäryhmä $\mathbb{R}_{a(N)}/\mathbb{R}_{a(N)}(1)$ on yksinkertainen.

Jatketaan normaalien aliryhmien muodostamista kiinnittämällä aina yksi nurkkapala enemmän. Kuten särmäpalojen kohdalla, tekijäryhmistä tulee aina yksinkertaisia. Lisäksi huomataan, että jos seitsemän nurkkapalaa on kiinnitetty, niin kahdeksas nurkkapala ei voi enää kääntyä kokonaiskiertymän säilymisehdon vuoksi (Häsä, 2010b: Korollaari 6.6.). Näin ollen on mahdollista kiinnittää ainoastaan kuusi nurkkapalaa. Siispä Rubikin nurkkapalojen asentoryhmän kompositiojonoksi saadaan

$$\mathbb{R}_{a(N)} \trianglerighteq \mathbb{R}_{a(N)}(1) \trianglerighteq \mathbb{R}_{a(N)}(2) \trianglerighteq \cdots \trianglerighteq \mathbb{R}_{a(S)}(6) \trianglerighteq 1,$$

jonka kaikki tekijät ovat kolmealkioisia yksinkertaisia syklisiä ryhmiä.

3.3 Rubikin ryhmän kompositiojono

Edellä sekä Rubikin paikkaryhmä $\mathbb{R}_p$ että asentoryhmä $\mathbb{R}_a$ pilkottiin pienimpiin mahdollisiin epätriviaaleihin normaaleihin aliryhmiin. Rubikin paikkaryhmän ja Rubikin särmäpalojen asentoryhmän tapauksessa kompositiojonot ovat vielä tekijäryhmissä. Kompositiojonoa halutaan tarkastella alkuperäisessä ryhmässä, joten tuodaan kyseiset jonot tekijäryhmistä takaisin Rubikin ryhmään $\mathbb{R}$. Tällaista operaatiota kutsutaan nostamiseksi.

Lause 3.13. *Olkoon $G_k \trianglerighteq G_{k+1}$ normaali jono ja kuvaus $\pi : G_k \to G_k/G_{k+1}$ kanoninen surjektio. Jos tekijäryhmällä G_k/G_{k+1} on epätriviaali aliryhmä*

H, niin sen alkukuvalle $\pi^{\leftarrow} H = \hat{H}$ pätee $G_k \trianglerighteq \hat{H} \trianglerighteq G_{k+1}$, ja hienonnetun jonon tekijät ovat edelleen epätriviaaleja.

Todistus. Tunnetusti normaalin ryhmän alkukuva kanonisessa surjektiossa on normaali kuvauksen lähtöjoukossa. Siispä $\pi^{\leftarrow} H = \hat{H} \trianglelefteq G_k$. Selvästi $G_{k+1} \subset \hat{H}$. Lisäksi, koska ryhmä G_{k+1} on normaali ryhmässä G_k, niin se on normaali myös pienemmässä ryhmässä $\hat{H}$. Näin ollen $G_k \trianglerighteq \hat{H} \trianglerighteq G_{k+1}$. Lisäksi $\hat{H} \neq G_k$, sillä $\pi \hat{H} = H \neq G_k/G_{k+1}$, ja $\hat{H} \neq G_{k+1}$, sillä $H \neq \{1\}$. Näin ollen hienonnetussa jonossa ei ole triviaaleja tekijöitä. $\square$

Nyt Rubikin paikkaryhmän kompositiojono

$$\mathbb{R}_p \trianglerighteq \mathbb{R}_p^{(1)} \trianglerighteq \mathbb{R}_{p(N)} \trianglerighteq 1,$$

voidaan nostaa takaisin Rubikin ryhmään tarkastelemalla aina kunkin normaalin aliryhmän alkukuvaa kanonisessa surjektiossa. Tunnetusti normaalin aliryhmän alkukuva kanonisessa surjektiossa on normaali aliryhmä. Merkitään nostettua normaalia aliryhmää $\hat{H}$ erotuksena tekijäryhmän alkiosta H. Nyt Rubikin paikkaryhmän kompositiojono on lopullisessa muodossaan

$$\mathbb{R} = \hat{\mathbb{R}}_p \trianglerighteq \hat{\mathbb{R}}_p^{(1)} \trianglerighteq \hat{\mathbb{R}}_{p(N)} \trianglerighteq 1.$$

Nostetaan vastaavasti Rubikin särmäpalojen asentoryhmän kompositiojono

$$\mathbb{R}_{a(S)} \trianglerighteq \mathbb{R}_{a(S)}(1) \trianglerighteq \mathbb{R}_{a(S)}(2) \trianglerighteq \mathbb{R}_{a(S)}(3) \trianglerighteq \cdots \trianglerighteq \mathbb{R}_{a(S)}(10) \trianglerighteq 1,$$

tekijäryhmästä Rubikin asentoryhmään kuten Rubikin paikkaryhmän tapauksessa. Rubikin asentoryhmän kompositiojonon muodostamisessa ollaan siis seuraavassa vaiheessa:

$$\mathbb{R}_a \trianglerighteq \hat{\mathbb{R}}_{a(S)} \trianglerighteq \hat{\mathbb{R}}_{a(S)}(1) \trianglerighteq \hat{\mathbb{R}}_{a(S)}(2) \trianglerighteq \hat{\mathbb{R}}_{a(S)}(3) \trianglerighteq \cdots \trianglerighteq \hat{\mathbb{R}}_{a(S)}(10) \trianglerighteq \mathbb{R}_a(N) \trianglerighteq 1.$$

Yhdistämällä edelliset tiedot Rubikin nurkkapalojen asentoryhmän kompositiojonon kanssa, koko Rubikin ryhmän kompositiojonoksi saadaan

$$\begin{aligned} \mathbb{R} &= \hat{\mathbb{R}}_p \trianglerighteq \hat{\mathbb{R}}_p^{(1)} \trianglerighteq \hat{\mathbb{R}}_{p(N)} \trianglerighteq \mathbb{R}_a \\ &\trianglerighteq \hat{\mathbb{R}}_{a(S)} \trianglerighteq \hat{\mathbb{R}}_{a(S)}(1) \trianglerighteq \hat{\mathbb{R}}_{a(S)}(2) \trianglerighteq \hat{\mathbb{R}}_{a(S)}(3) \trianglerighteq \cdots \trianglerighteq \hat{\mathbb{R}}_{a(S)}(10) \\ &\trianglerighteq \mathbb{R}_{a(N)} \trianglerighteq \mathbb{R}_{a(N)}(1) \trianglerighteq \mathbb{R}_{a(N)}(2) \trianglerighteq \cdots \trianglerighteq \mathbb{R}_{a(S)}(6) \trianglerighteq 1. \end{aligned}$$

Näin ollen Rubikin ryhmän kompositiotekijöitä on yhteensä 21 kappaletta ja ne ovat järjestyksessä

$$C_2, A_{12}, A_8, \underbrace{C_2, \ldots, C_2}_{\text{11 kpl}}, \underbrace{C_3, \ldots, C_3}_{\text{7 kpl}}.$$

Kompositiotekijöiden tunteminen mahdollistaa Rubikin ryhmän kertaluvun $|\mathbb{R}|$ eli kuution kaikkien mahdollisten asentojen lukumäärän selvittämisen. Kompositiojonon ominaisuuksien ja Lagrangen lauseen nojalla Rubikin ryhmän $|\mathbb{R}|$ kertaluku on nimittäin sen kompositiotekijöiden kertalukujen tulo. Alternoivan ryhmän A_n kertaluku on puolet vastaavan symmetrisen ryhmän S_n kertaluvusta, ja syklisen ryhmän C_n kertaluku on n. Edellisten tietojen nojalla koko Rubikin ryhmän $\mathbb{R}$ kertaluku on siis

$$\begin{aligned}|\mathbb{R}| &= |C_2| \cdot |A_{12}| \cdot |A_8| \cdot |C_2|^{11} \cdot |C_3|^7 \\ &= 2 \cdot \frac{12!}{2} \cdot \frac{8!}{2} \cdot 2^{11} \cdot 3^7 \\ &\approx 4{,}3 \cdot 10^{19}.\end{aligned}$$

Näin ollen Rubikin kuutiolla on yhteensä noin $4{,}3 \cdot 10^{19}$ mahdollista eri asentoa.

4 Lähteet

1. (Häsä, 2010a)
   Jokke Häsä. *Algebra II.* Luentomoniste. Matematiikan ja tilastotieteen laitos. Helsingin yliopisto. Kevät 2010. Saatavissa myös osoitteessa `http://www.cs.helsinki.fi/u/jhasa/kurssit/algebraII/materiaali.pdf`

2. (Häsä, 2010b)
   Jokke Häsä. *Ryhmäteoreettinen näkökulma Rubikin kuutioon.* Luentomoniste. Matematiikan ja tilastotieteen laitos. Helsingin yliopisto. Syksy 2010. Saatavissa myös osoitteessa `http://www.mv.helsinki.fi/home/jramo/Rubik_2010/materiaali_2010.pdf`.

3. (Rokicki et al., 2010)
   Tomas Rokicki et al. *God's Number is 20.* 2010. `http://www.cube20.org/`. Haettu 30. tammikuuta 2015.

4. (Tran, 2005)
   Raymond Tran. *A Mathematical Approach to Solving Rubic's Cube.* `http://www.math.ubc.ca/~cass/courses/m308/projects/rtran/rtran.pdf`. 2005. Haettu 30. tammikuuta 2015.

5. (WCA)
   World Cube Association. *Official Results.* `http://worldcubeassociation.org/results/regions.php`. Haettu 30. tammikuuta 2015.